Threat Intelligence

O que é, o que *não* é, como consumi-la corretamente

arcon
serviços gerenciados de segurança

INTRODUÇÃO

Nos últimos anos, temos presenciado, perplexos, um cenário assustador: cibercriminosos trabalhando e "inovando" a uma velocidade muito maior do que os provedores de defesas conseguem acompanhar. Temos visto a comercialização do cibercrime, com kits de malware e instruções detalhadas para realizar ataques sendo vendidos em comunidades clandestinas e vastas redes de botnets para ataques DDoS disponíveis para serem alugadas. Muitos cibercriminosos cooperam entre si, compartilhando códigos e informações para manterem seus artefatos maliciosos um passo à frente da indústria de cibersegurança.

É fundamental que a cibersegurança siga este mesmo caminho: **compartilhamento de informação.**

À medida em que mais e mais ataques ocorrem, aumenta a probabilidade de alguma organização ou grupo ter visto tal ataque antes. O conhecimento, portanto, existe de alguma forma, em algum lugar. Entretanto, precisa ser garimpado, validado e transformado em informação acionável. O objetivo da **Threat Intelligence** é fornecer a capacidade de reconhecer e atuar em tempo hábil sobre indicadores de comprometimento (*Indicators of Compromise – IOC*).

Existe uma consciência geral nas organizações da necessidade de se "ter" **Threat Intelligence**, porém ainda há muita confusão sobre o que é e como deve ser entregue e consumida.

Esse ***White Paper*** busca esclarecer o que realmente isso significa. A promessa é sedutora: ajudar as organizações a compreender e gerenciar o risco do negócio – dominar ameaças desconhecidas e mitigá-las, melhorando a eficácia da defesa cibernética.

O QUE É; O QUE **NÃO** É

Threat intelligence é informação específica sobre ameaças, gerada por alguma forma de processamento, tais como a coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências – incluindo contexto, mecanismos, indicadores e implicações – sobre uma ameaça, existente ou emergente, que coloque em perigo ativos de informação ou de tecnologia. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco.

Vemos muitas vezes o termo **Threat Intelligence** sendo empregado em contextos inadequados, talvez numa tentativa de valorizar algum tipo de informação que se pretenda divulgar. Entretanto, **Threat Intelligence não é**:

- informação óbvia, trivial ou evidente sobre uma ameaça, que um indivíduo não treinado seria capaz de discernir por si mesmo
- informação puramente sobre vulnerabilidades
- mera análise de tráfego de redes ou logs de segurança

COMO GERAR THREAT INTELLIGENCE?

O termo “inteligência” pode abranger diversos significados. No contexto aqui apresentado, inteligência é o conhecimento transmitido ou adquirido através de estudo, pesquisa ou experiência, fruto da associação de informações, normalmente disponíveis em diversas fontes e diferentes formatos. Podemos entender, portanto, que se trata do resultado de um processo, não de um mero conjunto de informações.

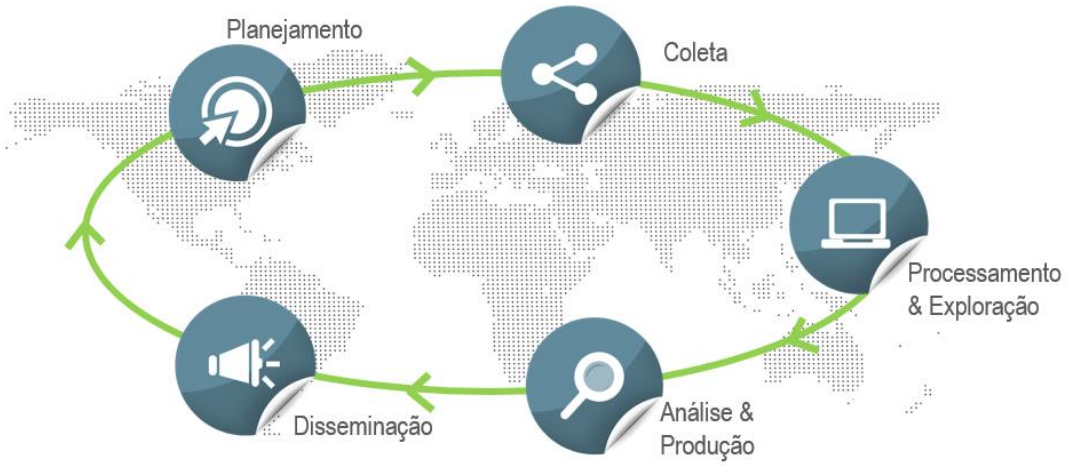

Fig.: Processo de geração de inteligência

Nas organizações, as equipes de cibersegurança têm à disposição múltiplas fontes de inteligência para identificar ameaças cibernéticas. Porém, os analistas de segurança acabam soterrados pela quantidade de informações e pela complexidade de operacionalizar e **transformar a inteligência em algo acionável**. É preciso muito esforço para separar o "joio do trigo", verificando e cruzando as fontes de inteligência, para transformar compreensão em ação.

O Gartner classifica o conteúdo de **Threat Intelligence** em 2 tipos, não sendo raro, entretanto, encontrar inteligência que misture os dois: conteúdo proveniente de aquisição e análise (*acquisition and analysis content*) e conteúdo em tempo real para monitoramento e notificação (*real-time monitoring and notification content*). O primeiro é tipicamente composto de análise narrativa contendo algum tipo de conteúdo antecipatório, com *insight* sobre os motivos e possíveis ações futuras do cibercriminoso. Naturalmente, este tipo de inteligência contém algum grau de incerteza, sendo útil no planejamento de orçamentos e estratégias de defesa. O segundo tende a ser mais técnico, sendo elaborado a partir de fontes com informações sobre a atividade operacional, que já ocorreu em algum lugar do mundo. Feeds de endereços IPs controladores de botnets são um exemplo deste tipo de inteligência, que tende a ser determinístico e confiável, fornecendo agilidade para ações e respostas em curto espaço de tempo. Normalmente é entregue na forma de *Machine-Readable Threat Intelligence* (MRTI), que nada mais é do que **Threat Intelligence** em um formato compreendido por máquinas. É, portanto, o conhecimento consolidado a partir de grandes quantidades de informações, provendo contexto para suportar ações táticas e, por vezes, estratégicas, para equipes de cibersegurança. Está pronta para ser empregada em diversas tecnologias de segurança, seja na nuvem ou na infraestrutura *on-premises*, pois já foi traduzida de "linguagem humana" para um formato *machine-readable*.

Tratar tamanho volume de dados, com uma variedade virtualmente ilimitada de fontes de inteligência sobre ameaças, gerada tanto externa quanto internamente, tanto em formato estruturado quanto desestruturado, requer a utilização de uma plataforma específica para isto. As *Threat Intelligence Platforms* (TIP), dotadas de capacidade de lidar com big-data e *analytics*, devem ser capazes de enriquecer e correlacionar essa inteligência sobre ameaças e possibilitar a geração da MRTI para alimentação de tecnologias como SIEM, sistemas de prevenção de intrusão (IPS), firewalls de próxima geração (NGFW) e gateways de web.

COMO UTILIZAR THREAT INTELLIGENCE?

Um cenário de ataque por ameaças avançadas pode levar-nos a fazer perguntas como: "quem nos tem como alvo?", "que métodos estão usando?", "que informações estão buscando?". Ter claro o que se quer saber sobre atores de ataques e seus métodos e como prevenir ou detectar ataques pode ajudar imensamente quando planejamos políticas e ações de defesa.

A utilização de **Threat Intelligence** pode reduzir significativamente a quantidade de incidentes de segurança, bem como aumentar dramaticamente a velocidade de resposta aos incidentes detectados. Isto acontece graças à redução de falso-positivos pela validação baseada em vários critérios, o que ajuda a oferecer visão, contexto e credibilidade no que diz respeito à informação que está sendo observada, como, por exemplo, se estamos tratando de um ataque isolado ou parte de um ataque direcionado amplamente a uma vertical de mercado.

Para muitas organizações que utilizam **Threat Intelligence**, um desafio fundamental é **como consumir e como agir sobre essa inteligência**. Ela pode ser usada de forma estratégica, para lastrear decisões sobre a preparação para uma ameaça, como forma de evitar ou reduzir o seu impacto potencial. Também pode ser usada de forma tática, para responder a um incidente decorrente da ameaça, nas tarefas de identificação, avaliação, suporte forense e remediação.

Threat Intelligence Estratégica → tipicamente consumida pelo *C-level* de uma organização. Sua finalidade é ajudar a compreender riscos correntes e a identificar outros riscos potenciais. Trata de conceitos de alto nível de risco e probabilidades, ao invés de aspectos técnicos, para orientar as decisões estratégicas de negócios. Normalmente é apresentada como relatórios ou *briefings*.

Threat Intelligence Tática → informação sobre como atores de ameaças (*threat actors*) estão realizando ataques; que ferramentas, técnicas e processos (*tools, techniques and processes – TTPs*) estão sendo utilizados. É consumida por defensores e times de resposta a incidentes, para garantir que seus mecanismos de defesa, alertas e investigação estão preparados para as táticas de ataque atuais. Este tipo de inteligência muitas vezes tem uma vida curta, já que os atores podem facilmente alterar os endereços IP de origem ou modificar *hashes* de arquivos. Daí a necessidade de consumir tal inteligência de forma automatizada e de atualizá-la com enorme frequência.

Referências:

- “Technology Overview for Threat Intelligence Platforms” - Gartner | Dezembro de 2014
- “How Gartner Defines Threat Intelligence” - Gartner | Fevereiro de 2016
- “Innovation Insight for Machine-Readable Threat Intelligence” - Gartner | Março de 2016

Sobre a Arcon

Atuando no mercado nacional desde 1995, a Arcon é especializada em segurança de TI com foco em serviços gerenciados de segurança (MSS – Managed Security Services). Com um completo portfólio e sólidas parcerias com os principais fabricantes do mundo, a empresa monitora e gerencia ambientes, mitiga os riscos e previne incidentes em empresas de grande porte. A partir de seus SOCs, a Arcon processa +2 bilhões de eventos por dia, protege mais de 600.000 ativos e possui inteligência de segurança única na América Latina.

É a única empresa de serviços gerenciados de segurança no ranking Exame PME 2015 das empresas que mais crescem no Brasil. Nos últimos anos, firmou-se como líder no mercado brasileiro de MSS, tendo conquistado, o primeiro lugar em MSS no ranking Anuário Outsourcing por 4 anos consecutivos. www.arcon.com.br

São Paulo

Av. Ibirapuera, 2.332 | 5º andar
04.028-002 . Moema
Tel: 11 3525-1800

Rio de Janeiro

Av. Presidente Vargas, 3.131 | 16º andar
20.210-911 . Cidade Nova
Tel: 21 3293-1000

Brasília

SCN Qd.02 Bl A | 5º andar
70.712-900
Tel: 61 3329-6081

Belém

Av. Gov. José Malcher, 937 | 5º andar
66.055-260 . Nazaré
Tel: 91 3210-2308

www.arcon.com.br